NISTTech

Interactive Analysis of Attack Graphs using Relational Queries

Defend against computer network intrusions

Description

To help safeguard valuable information most efficiently, computer scientists at NIST have applied security metrics to computer network pathways to assign a probable risk of attack to guide IT managers in securing their networks. Once inside a network's firewall, a hacker can travel through the network through a variety of routes to hit the jackpot of valuable data. In addition to hardware, the hacker can break in through software on the computers, especially file-sharing applications that have been blamed for some major data breaches recently. All of the paths that system attackers could penetrate through a network are analyzed using the NIST technique and a risk factor is assigned to each component of the system. Decision makers can use these assigned probabilities to make wise decisions and investments to safeguard their network. NIST researchers evaluate each route and assign it a risk based on how challenging it is to the hacker. The paths are determined using a technique called "attack graphs." This NIST technology can be packaged as software to be marketed as a risk analysis tool to secure networked resources.

Applications

- **Computer network safety**
  Identify and prioritize pathway threats leading to breaches.

Advantages

- **Speed**
  Greater speed in identifying attack mechanisms.
- **Interactive analysis of attack graphs**
  Dynamically construct and revise relational queries.

Abstract

Attack graph is important in defending against we II-orchestrated network intrusions. However, the current analysis of attack graphs requires an algorithm to be developed and implemented, causing a delay in the availability of analysis. Such a delay is usually unacceptable because the needs for analyzing attack graphs may change rapidly in defending against network intrusions. An administrator may want to revise an analysis upon observing its outcome. Such an interactive analysis,

similar to that in decision support systems, is difficult if at all possible with current approaches based on proprietary algorithms. This paper removes the above limitation and enables interactive analysis of attack graphs. We devise a relational model for representing necessary inputs including network configuration and domain knowledge. We generate the attack graph from those inputs as relational views. We then show that typical analysis of the attack graph can be realized as relational queries against the views. Our approach eliminates the needs for developing a proprietary algorithm for each different analysis, because an analysis is now simply a relational query. The interactive analysis of attack graphs is now possible, because relational queries can be dynamically constructed and revised at ru time. Moreover, the mature optimization techniques in relational databases can also improve the performance of the analysis.

Inventors

- Singhal, Anoop
- Jajodia, Sushil
- Wang, Lingyu
- Yao, Chao

Citations

1. L. Wang, T. Islam, T. Long, A. Singhal and S. Jajodia. An Attack Graph Based Probabilistic Security Metric. IFIP WG 11.3 Conference on Data and Application Security, London, United Kingdom.
2. L. Wang, A. Singhal, S. Jajodia. Toward Measuring Network Security Using Attack Graphs. Proc. of the 2007, ACM workshop on Quality of protection, pp 49-54, Oct 07.
3. L. Wang, C. Yao, A. Singhal, S. Jajodia. Interactive analysis of attack graphs using relational queries. Lecture Notes in Computer Science (2006) Volume: 4127, Publisher: Springer, Pages: 119-132.

Related Items

- Article: How Secure Is Your Network? NIST Model Knows

References

- U.S. Patent Application # 20080046393
- Docket: 07-001

Status of Availability

This invention is available for licensing.

Last Modified: 01/13/2010